National Infrastructure Protection Center
CyberNotes

Issue #2001-23 *November 19, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between October 30 and November 16, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Acme Software[1]	Unix	mini_httpd 1.10-1.15; thttpd 1.90a-2.21	A vulnerability exists due to the way the httpd daemon handles file requests, which could let a remote malicious user access restricted information.	**THTTPD Secure Webserver 2.22:** http://www.acme.com/software/thttpd/ **Mini_HTTPD Webserver 1.16:** http://www.acme.com/software/mini_httpd/	THTTPD/ Mini_HTTPD File Disclosure	Medium	Bug discussed in newsgroups and websites. Vlnerability can be exploited via a web browser.

[1] Cgi Security Advisory #6, November 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Active state[2]	Windows	ActivePerl 5.6.1	A buffer overflow vulnerability exists in 'perlIIS.dll' module, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.activestate.com/Products/ActivePerl/download.plex	ActivePerl perlIIS.dll Buffer Overflow CVE Name: CAN-2001-0815	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Apache[3]	Multiple	Apache 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20	A vulnerability exists due to the way the 'mod_usertrack' module issues authentication IDs. Any applications that rely on these IDs for authentication may be vulnerable to ID prediction attacks.	No workaround or patch available at time of publishing.	Apache mod_usertrack Predictable ID Generation	Medium	Bug discussed in newsgroups and websites.
Caldera[4]	Unix	OpenUnix 8.0; UnixWare 7	A buffer overflow vulnerability exists due to improper bounds checking in the ToolTalk library, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://stage.caldera.com/pub/security/openunix/CSSA-2001-SCO.29/erg711780.Z	ToolTalk Library Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Carnegie Mellon University[5]	Unix	Cyrus-SASL 1.5.24, 1.5.25, 1.5.26	A format string vulnerability exists in the Simple Authentication and Security Layer (SASL), which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/BETA/cyrus-sasl-1.5.27.tar.gz	Cyrus-SASL Syslog Format String	**High**	Bug discussed in newsgroups and websites.
Cisco Systems[6]	Multiple	IOS 12.0ST, IOS 12.0S	Six vulnerabilities involving Access Control List (ACL) exist in multiple releases of Cisco IOSR Software Release for Cisco 12000 Series Internet Routers. Not all vulnerabilities are present in all IOS releases and only line cards based on the Engine 2 are affected by them. These vulnerabilities could cause a Denial of Service, circumvent the protection offered by ACL, or cause unwanted traffic to be allowed in and out of the protected network. The security based on an ACL will be breached completely.	Upgrade available at: http://www.cisco.com	Cisco Multiple Access Control Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. Some of these vulnerabilities do not require an exploit code and some can be exploited via a web browser.

[2] NSFOCUS Security Advisory, SA2001-07, November 15, 2001.

[3] SecurityFocus, November 9, 2001.

[4] Caldera Security Advisory, CSSA-2001-SCO.29, November 2, 2001.

[5] Securiteam, November 3, 2001.

[6] Cisco Security Advisory, November 14, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[7]	Multiple	IOS 12.0ST, 12.0SC, 12.0S	Denial of Service vulnerability exists if circumstances require an affected router to send out a large of number of ICMP unreachable packets.	Upgrade available at: http://www.cisco.com	Cisco 12000 Series Internet Router Denial Of Service	High	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Cisco Systems[8]	Multiple	IOS 11.1-12.2	A Denial of Service vulnerability exists because it is possible to send an Address Resolution Protocol (ARP) packet on a local broadcast interface.	Upgrade available at: http://www.cisco.com	Cisco Local Interface ARP Denial of Service	High	Bug discussed in newsgroups and websites.
Duncan Hall[9]	Unix	Viralator 0.7, 0.8, 0.9pre1	A vulnerability exists because filenames taken from an URL are not validated, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Viralator CGI Input Validation Remote Shell Command	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Entrust[10]	Multiple	GetAccess 1.0	A vulnerability exists in the default shellscripts because user-supplied input is not validated, which could let a malicious user obtain sensitive information.	Patch available at: https://login.encommerce.com/private/docs/techSupport/Patches-BugFix	GetAccess File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
e-Zone Media Inc.[11]	Windows NT	FuseTalk 2.0, 3.0	A vulnerability exists in the 'join.cfm' form due to improper form sanitization, which could let a malicious user execute malicious SQL.	Patch available at: http://www.e-zonemedia.com/upgrade.cfm?productid=1	FuseTalk Form Input Validation	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Flicks Software[12]	Windows	Titan 5.5a	A vulnerability exists because escaped characters are not decoded, which could let a malicious user bypass security rules.	No workaround or patch available at time of publishing.	Titan Application Firewall Escaped Character Decoding	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Francisco Burzi[13]	Multiple	PHP-Nuke 5.2	A vulnerability exists in 'admin/case/case.filemanager.php', which could let a remote malicious user copy and delete arbitrary files on the server	No workaround or patch available at time of publishing.	PHP Nuke Copying and Deleting Files	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[7] Cisco Security Advisory, November 14, 2001.
[8] Cisco Security Advisory, November 15, 2001.
[9] Securiteam, November 4, 2001.
[10] Entrust Security Bulletin, E01-005, November 5, 2001.
[11] Securiteam, November 4, 2001.
[12] SecurityFocus, November 16, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Horde Project[14]	Unix	IMP 2.0, 2.2-2.2.6	A vulnerability exits in 'status.php3', which could let a remote malicious user execute arbitrary code.	Upgrade to Horde IMP 3.0 available at: http://www.horde.org/imp/3.0	IMP Session Hijacking	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[15]	Windows NT 4.0, Unix	HTTP Server 1.3.3 win32, 1.3.6win32, 1.3.6.4 win32, 1.3.6.3, 1.3.6.2 win32, 1.3.6.2 unix, 1.3.12.4, 1.3.12.3, 1.3.12.2, 1.3.19	A vulnerability exists due to an input validation error, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	IBM HTTP Server Source Code Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Ipswitch[16]	Windows NT 4.0/2000	WS FTP Server 1.0.1-2.0.3	A buffer overflow vulnerability exists when a specially crafted FTP command is submitted, which could let a malicious user execute arbitrary code.	Patch available at: ftp://ftp.ipswitch.com/Ipswitch/Product_Support/WS_FTP_Server/ifs204.exe	WS_FTP Server 'STAT' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[17]	Windows 2000	Windows 2000, 2000 SP1&SP2	A Denial of Service vulnerability exists if a malicious user were to create a named pipe session without requesting any service.	The fix for this vulnerability will be included in Service Pack 3.	Windows 2000 RunAs Service Denial of Services	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[18]	Windows 2000	Windows 2000, 2000 SP1&SP2	A vulnerability exists when the RunAs service is invoked because it creates a named pipe for client for communication of credentials (in cleartext), which could let a malicious user obtain sensitive information.	The fix for this vulnerability will be included in Service Pack 3.	Windows 2000 RunAs Service Named Pipe Hijacking	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[19]	Windows 2000	Windows 2000, 2000 SP1&SP2	A vulnerability exists because the username and password are stored in cleartext in memory, which could let a malicious user obtain sensitive information.	The fix for this vulnerability will be included in Service Pack 3.	Windows 2000 RunAs User Credentials Exposure	Medium	Bug discussed in newsgroups and websites.
Microsoft[20]	Windows 2000	Windows XP, 2000, 2000 SP1&SP2	A vulnerability exists in Terminal Service, which could allow a malicious user to have a false IP address logged.	No workaround or patch available at time of publishing.	Microsoft Windows Terminal Services False IP Address	Medium	Bug discussed in newsgroups and websites.

[13] Magnux Software Advisory, MASA:01-02:en, November 5, 2001.
[14] Bugtraq, November 9, 2001.
[15] Bugtraq, November 8, 2001.
[16] Defcom Labs Advisory def-2001-31, November 5, 2001.
[17] Team RADIX Research Report, RADIX1112200103, November 12, 2001.
[18] Team RADIX Research Report, RADIX1112200101, November 12, 2001.
[19] Team RADIX Research Report, RADIX1112200102, November 12, 2001.
[20] Xato Network Advisory, XATO-112001-01, November 7, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[21]	Windows 95/98/NT 4.0/2000	Internet Explorer 5.01, 5.0.1SP1&2, 5.5, 5.5SP1&2	A vulnerability exists in Internet Explorer, which could allow a web site to be viewed in the Local Intranet Zone (rather than the Internet Zone) and run with fewer security restrictions than appropriate. This is a new variant of a vulnerability discussed in Microsoft Security Bulletin MS01-051 affecting how IE handles URLs that include dotless IP addresses.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-055.asp	Microsoft Internet Explorer Zone Spoofing CVE Name: CAN-2001-0664	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[22]	Windows 98/98/ME/ NT 3.5/3.5.1/ 4.0/2000	Internet Explorer 5.5, 5.5 SP1&SP2, 6.0	Two vulnerabilities exist due to the way IE handles cookies across domains, which could let a malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-055.asp	Microsoft Internet Explorer Cookie Vulnerabilities CVE Name: CAN-2001-0722, CAN-2001-0723	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Miquel van Smoorenburg[23]	Multiple	Cistron Radius 1.6.4	A buffer overflow vulnerability exists in a function that is used to calculate a message digest, which could let a remote malicious user cause a Denial of Service.	Upgrade available at: http://www.radius.cistron.nl/	Cistron Radius Digest Calculation Buffer Overflow	Low	Bug discussed in newsgroups and websites.

[21] Microsoft Security Bulletin, MS01-055, November 13, 2001.
[22] Microsoft Security Bulletin, MS01-055, November 13, 2001.
[23] Bugtraq, November 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[24]	Unix	Caldera OpenUnix 8.0, UnixWare 7; Compaq Tru64 5.0, 5.1; HP-UX 10.10, 10.20, 11.0, 11.11, HP-UX (VVOS) 10.24, 11.0.4; IBM AIX 4.0- 5.1; Open Group CDE Common Desktop Environment 1.0.1-2.1; SGI IRIX 6.1-6.5.13; Sun Solaris 2.4-8.0, Sun Solaris 2.4 _x86-8.0 _x86; Xi Graphics DeXtop 2.1, Xi Graphics Maximum CDE 1.2.3	A buffer overflow vulnerability in one of the CDE components, which could let a remote malicious user gain administrative privileges.	**Caldera:** ftp://stage.caldera.com/pub/security/openunix/CSSA-2001-SCO.30/erg711881.Z **HP-UX:** ftp://dtspcd:dtspcd@hprc.external.hp.com/dtspcd.tar.gz **HP-UX (VVOS):** ftp://dtspcd:dtspcd@hprc.external.hp.com/dtspcd.tar.gz	CDE dtspcd Overflow CVE Name: CAN-2001-0803	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[25], [26], [27], [28]	Unix	Linux kernel 2.0-2.0.39, 2.2-2.2.20, 2.4-2.4.13	A vulnerability exists in the packet filter, which could let a malicious user circumvent certain types of firewall configurations and access restricted services.	**Caldera:** ftp://ftp.caldera.com/pub/updates/ **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/ **RedHat:** ftp://updates.redhat.com/ **EnGarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/	Linux Syn Filter Evasion	Medium	Bug discussed in newsgroups and websites.
NRL[29]	Unix	OPIE 2.4, 2.32	An information leakage vulnerability exists in combined OpenSSH and S/Key implementations, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	OPIE Account Existence Information Leak	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[24] CERT® Advisory CA-2001-31, November 13, 2001.
[25] Caldera Security Advisory, CSSA-2001-038.0, November 5, 2001.
[26] SuSE Security Announcement, SuSE-SA:2001:036, November 2, 2001.
[27] Red Hat Security Advisory, RHSA-2001:142-15, November 2, 2001.
[28] EnGarde Secure Linux Security Advisory, ESA-20011106-01, November 6, 2001.
[29] Securiteam, November 16, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Opera Software[30]	Windows 95/98/ME/ NT 4.0/2000, Unix	Opera Web Browser 5.02 win32, 5.0 Linux, 5.11 win32, 5.10 win32, 5.12 win32	A cross-site scripting vulnerability exists because the "Same Origin Policy" is not properly implemented, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Opera Cross-Site Scripting	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Progress Software[31]	Windows NT 4.0/2000, Unix	Progress Database 9.1C	A format string vulnerability exists because the 'PROMSGS' utility incorrectly parses the input file, which could let a malicious user gain execute arbitrary code.	No workaround or patch available at time of publishing.	Progress Database Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Rational[32]	Unix	ClearCase 3.2, 4.0-4.2	A vulnerability exists in the way environment variables are handled by 'db_loader', which could let a malicious user execute arbitrary code and gain administrative access.	No workaround or patch available at time of publishing.	ClearCase Ddb_loader Term Environment Variable Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
RedHat[33]	Unix	TUX 2.1.0-2	A Denial of Service vulnerability exists when the TUX daemon receives an oversized Host: header as part of a HTTP request.	Upgrade available at: ftp://updates.redhat.com/	TUX HTTP Server Oversized Host Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[34]	Unix	Linux 7.1k i386	A vulnerability exists due to the implementation of umask used in some Korean installation programs, which could let a malicious user gain elevated privileges.	Upgrade available at: ftp://updates.redhat.com/7.1/kr/os/	Linux Korean Installation Insecure Default UMask	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
RedHat[35]	Unix	Linux 7.1 i386, alpha, 7.2 i386	A vulnerability exists in the firewall infrastructure included with the Operating System, which could let a remote malicious user access restricted resources.	Update available at: ftp://updates.redhat.com/	Linux IPTables Save Option Unrestorable Rules	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Rick Fournier[36]	Multiple	Network Tools 0.2	A vulnerability exists when a command encapsulated in metacharacters is passed to the modules in the suite, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Network Tool PHPNuke Addon Metacharacter Filtering Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Slashcode[37]	Multiple	Slashcode 2.0	A vulnerability exists if users do not change their initial session ID password, which could let a malicious user gain unauthorized access.	No workaround or patch available at time of publishing.	Slashcode Guessable SessionID	Medium	Bug discussed in newsgroups and websites.

[30] Georgi Guninski Security Advisory #51, November 15, 2001.
[31] Securiteam, November 7, 2001.
[32] Bugtraq, November 9, 2001.
[33] Red Hat Security Advisory, RHSA-2001:142-15, November 2, 2001.
[34] Red Hat Security Advisory, RHSA-2001:148-09, November 13, 2001.
[35] Red Hat Security Advisory, RHSA-2001:144-04, November 5, 2001.
[36] Bugtraq, November 16, 2001.
[37] SecurityFocus, November 8, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sleepycat Software[38]	Unix	Sleepycat Software db 2.7.7	A vulnerability exists due to a configuration mistake in the 'libdb1' package, which could let a remote malicious user obtain elevated privileges or a local malicious user gain root access.	Upgrade available at: ftp://ftp.caldera.com/pub/updates/OpenLinux/3.1/Server/current/	LibDB SNPrintF Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sun Micro Systems, Inc.[39]	Unix	Solaris 8.0_x86, 8.0	A vulnerability exists in the way access control entries are handled, which could let a malicious user write to another terminal.	No workaround or patch available at time of publishing.	Solaris PT_CHMOD Arbitrary Terminal Writing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec[40]	Windows NT 4.0, Unix	Raptor Firewall 4.0.0 HP-UX; 5.0.3 Windows NT, 6.0.2 Windows NT, 6.0.2 Windows NT, 6.5 Windows NT; Veloci Raptor 1.0, 1.1	A remote Denial of Service vulnerability exists when the firewall receives zero length UDP packets.	Upgrade to a version greater than 6.5.	Raptor Firewall Zero Length UDP Packet Resource Consumption	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Wietse Venema[41]	Multiple	Postfix 20010228, 19991231, 19990906	A Denial of Service vulnerability exists if the client-server SMTP conversation log becomes too large.	Patch available at: http://www.securityfocus.com/data/vulnerabilities/patches/postfix2001.patch	Postfix SMTP Log Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[38] Caldera Security Advisory, CSSA-2001-037.0, October 30, 2001.
[39] SecurityFocus, November 9, 2001.
[40] SecurityFocus, November 5, 2001.
[41] Bugtraq, November 15, 2001.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 5 and November 13, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 9 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	**Script Name**	**Script Description**
November 13, 2001	Hp-ux-bdf.c	Script which exploits the buffer overflow vulnerability in HP-UX's /usr/bin/bdf.
November 12, 2001	**Radix1112200103.C**	**Script which exploits the Windows 2000 RunAs Service Denial of Services vulnerability.**
November 12, 2001	**Radix1112200101.C**	**Script which exploits the Windows 2000 RunAs Service Named Pipe Hijacking vulnerability.**
November 12, 2001	Ettercap-0.6.2.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
November 9, 2001	**Clearcase_x86exp.C**	**Script which exploits the Rational ClearCase DB Loader TERM Environment Variable Buffer Overflow vulnerability.**
November 6, 2001	Flawfinder-0.17.tar.gz	Flawfinder searches through source code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first.
November 5, 2001	Iis5-koei.zip	Script which exploits the null.printer buffer overflow vulnerability.
November 5, 2001	Raptor-dos.pl	Perl script which exploits the Raptor Firewall Zero Length UDP Packet Resource Consumption vulnerability.
November 5, 2001	Ws_ftp2.0.3.pl	Perl script which exploits the Ipswitch WS_FTP Server 'STAT' Buffer Overflow vulnerability.

Trends

Probes/Scans:

- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**
- **CERT/CC is receiving reports of increased scanning activity for the SSH service (22/tcp). For more information, see CERT® Incident Note IN-2001-12, located at: http://www.cert.org/incident_notes/IN-2001-12.html.**

Other:

- **NIPC has reason to believe that the potential for future DDoS attacks is high. Protesters have indicated they are targeting web sites of the U.S. Department of Defense and organizations that support the critical infrastructure of the United States. For more information, see NIPC ADVISORY 01-026 located at: http://www.nipc.gov/warnings/advisories/2001/01-026.htm.**
- **The National Infrastructure Protection Center (NIPC) continues to observe hacking activity targeting the e-commerce or e-finance/banking industry. For more information, see NIPC ADVISORY 01-023 located at: http://www.nipc.gov/warnings/advisories/2001/01-023.htm. The most prevalent exploit being used to gain access to targeted systems is the Unicode vulnerability**

found in the Microsoft Internet Information Services (IIS) web server software, http://www.microsoft.com/technet/treeview/default.asp?url=/technet.security/bulletin/MS00-086.asp.

- **The National Infrastructure Protection Center expects to see an upswing in incidents as a result of the tragic events of September 11, 2001. For more information, see NIPC ADVISORY 01-020, available at http://www.nipc.gov/warnings/advisories/2001/01-020.htm.** Also, the FBI's computer crime division is warning Americans to expect an increase in cyber protests and "hacktivism" in the wake of the U.S. response to the Sept. 11 terrorist attacks. For more information, see "Cyber Protest: The Threat to the U.S. Information Infrastructure," located at: http://www.nipc.gov/cyberprotests.pdf.
- **CERT/CC has received multiple reports of systems being compromised via the CRC-32 compensation attack detector vulnerability. For more information, see CERT® Incident Note IN-2001-12, located at: http://www.cert.org/incident_notes/IN-2001-12.html.**
- **CERT has released a statement concerning multiple vulnerabilities in several implementations of the line printer daemons of several types of systems. These holes would allow intruders to gain root privileges and launch Denial of Service attacks through IBM AIX line printers, FreeBSD, netBSD, openBSD and Hewlett-Packard Co. HP-UX line printers. For more information, see CERT Advisory CA-2001-30, located at: http://www.cert.org/advisories/CA-2001-30.html.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/SirCam	Worm	Slight Increase	July 2001
2	W32/Nimda	File, Worm	Slight Decrease	September 2001
3	W32/Magistr-(A &B)	File, Worm	Stable	March 2001
4	W32/Hybris	Worm	Slight Increase	November 2000
5	VBS/Haptime	Script	Slight Increase	May 2001
6	W32/Funlove	File	Slight Increase	November 1999
7	VBS/Kakworm	Script	Slight Increase	December 1999
8	W32/Apology (MTX)	File Infector, Trojan	Return to Table	September 2000
9	W32/BadTrans	Worm	Return to Table	April 2001
10	VBS/Loveletter	Script	Return to Table	March 2000

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **201** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **463** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

BAT.Sakura (DOS Virus): This is a harmless parasitic script virus. The virus itself is a script program in BATCH for DOS language. The virus searches for .BAT files in the current and system directories, and writes itself to the end of them. The virus also appends text strings to the end of the system files. The virus erases .DOC files in the directory C:\WINDOWS\. It also deletes all files in the directories C:\ARCHIV~1\NAPSTER and C:\ANTVIRUS.

VBS_PILA.A (Aliases: I-Worm.Pila, Pilantra.i-worm, Pilantra virus) (Visual Basic Script Worm): This Internet worm spreads copies of itself via e-mail in Microsoft Outlook, via Internet Relay Chat (mIRC), and via mapped local and network drives. Similar to known VBS worms, it arrives as the following attachment in an e-mail, PLATÔNICO.TXT.SHS. Upon execution, it invokes the notepad application to display a text file containing a sexually explicit tale written in Portuguese. This worm also installs an IRC Backdoor, IRC_PILA.A.

W32/Finaldo-B (Aliases: W32/Finaldo.B@mm, Finaldoom) (Win32 Executable File Virus): This virus spreads by infecting files and web pages and also as an e-mail attachment. When an infected file is run it will create a hidden file named finaldoom.dll in the system's temporary directory. Finaldoom.dll is then loaded and it begins the infection process. The virus searches for files with .EXE, .SCR and .OCX extensions in order to infect them. It also searches for files with the extensions .HTM, .HTML and .ASP. If it finds such a file the virus will attempt to add malicious JavaScript to the file. If a webpage containing the malicious script is viewed, a file called finaldoom.eml is automatically downloaded onto the user's computer which is then executed, spreading the infection. The virus also searches the user's mailbox for addresses to which it can e-mail itself. The e-mail messages it sends have an attachment named ".EXE" and attempt to exploit a MIME Vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer to allow the executable file to run automatically without the user double-clicking on the attachment. Microsoft has also issued a patch which secures against the incorrect MIME header vulnerability which can be downloaded from http://www.microsoft.com/technet/security/bulletin/MS01-020.asp.

W32.Funsoul@mm (Win32 Worm): This is a worm that spreads by sending e-mail to contacts in the Microsoft Outlook address book. It will not execute properly if a printer is not connected to the computer. When executed, W32.Funsoul@mm does the following:

- It creates the files:
  - C:\Protect.sys
  - C:\Help.bat
  - C:\Hide.bat
  - C:\Login.scr
  - C:\Funny.scr
- It overwrites the C:\Autoexec.bat file with code that causes the dialer to dial 911 when you start the computer.
- It adds the value, "help C:\help.bat," to the registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- It adds the value, "HereAlso C:\Login.scr," to the key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

The worm sends itself to all contacts in the Microsoft Outlook address book. The e-mail has the following characteristics:

- Subject: Though you might find this funny !
- Attachment: Funny.scr

The worm also changes the Internet Explorer home page to a Web page that is dedicated to Timothy McVeigh. It then displays a message and Timothy McVeigh's picture.

W32/Klez-C, W32/Klez-D (Win32 Worm): This is a minor variant of the W32/Klez worm. They both carry a compressed copy of the W98/Elkern virus, which is dropped and executed when the worm is run. The worm sends itself to entries in the Windows address book and arrives in an e-mail with a random subject line. The attachment has a random filename and the sender address is either a random uppercase name at yahoo.com, hotmail.com or sina.com, or one chosen from a list inside the virus. The body text of the e-mail is sent as HTML and says:

> "I'm sorry to do so, but it's helpless to say sorry.
> I want a good job, I must support my parents.
> Now you have seen my technical capabilities.
> How much my year-salary now? NO more than $5,500.
> What do you think of this fact?
> Don't call my names, I have no hostility.
> Can you help me?"

The worm attempts to exploit a MIME vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer to allow the executable file to run automatically without the user double clicking on the attachment. Microsoft has issued a patch which secures against this vulnerability which can be downloaded from http://www.microsoft.com/technet/security/bulletin/MS01-020.asp. The worm copies itself to remote shares on other machines with random filenames. It also copies itself to the Windows System directory as krn132.exe, and sets the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\ Run\krn132 to point to that file.

W32.Paukor.B@mm (Win32 Worm): This is a worm that logs keystrokes to send to a malicious user and uses Microsoft Outlook to e-mail itself. The e-mail subject is "Pictures with your loved one," and the attachment is: "Images_zipped.exe."

W32/Redesi-H (Alias: mIRC/Redesi-H) (Win32 Worm): This is a worm which spreads using Microsoft Outlook and the mIRC (Internet Relay Chat) client. The worm arrives in an e-mail with a subject randomly chosen. Every message sent by the worm contains two attachments. One attachment is always a non-viral image in JPEG format named erica.jpg. The other attachment is the worm with a filename randomly chosen from a list. When run, the worm sends itself to every contact found in the user's Microsoft Outlook address book. It then changes the registry key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run so that it runs on Windows startup. The worm also attempts to create a mIRC script file C:\mirc\script.ini. The dropped script file tries to send the worm to other mIRC users. On every Friday, the worm displays a message box containing the text:

> "Erica, what sunshine is to flowers, your smiles are to happiness."

W32.Viled.gen (Alias: W32.Viled@mm) (Win32 File Worm): This worm sends itself to e-mail addresses in the Microsoft Outlook address book. The message has the following characteristics:

- Subject: A Little Bit Stupid But Good
- Message: Check This Out. Probably The Most Stupidest Thing I Ever Seen
- Attachment: thedevil.exe

W97M.Death.C (Word 97 Macro Virus): This is a Microsoft Word macro virus that infects the Normal.dot template and the active document. It also keeps track of how many times it has run on the computer. When activate is creates the directory structure, \Windows\Application Users\AddFile, on the currently active drive. It then creates the following files in the \AddFile folder:

- Pesquisa de Opiniao.doc
- Death Kiss.Ini

Next, the virus reads a number from the Death Kiss.Ini file and increments the number by one. The number equals how many times the virus has run on the computer. Finally, W97M.Death.C attempts to infect the Normal.dot template file and the active document

W97M_DED.R (Alias: DED.R) (Word 97 Macro Virus): This macro virus infects Word documents and document templates that are opened or closed, and then changes some system settings. It uses the C:\EVOLVE.TMP file to export its virus code into target files. It deletes this file after use. It intercepts the auto macros Document_Open and Document_Close and does not reinfect previously infected global templates that contain its virus code. When the global template is infected, it infects active Word documents that are opened thereafter. This virus changes the Document Summary Info of an infected file to the following:

.Title = "Ethan Frome"
.Author = "EW/LN/CB"
.Keywords = "Ethan"

WM97/Footer-AB (Word 97 Macro Virus): This is a Word macro virus. It generates two files in the root directory named footer.$$$ and footer.$$1. Both files contain copies of the macro virus code.

WM97/Goodday-C (Word 97 Macro Virus): This is a Word macro virus which infects Microsoft Word documents and templates. The virus does little more than spread and contains no malicious payload.

WM97/Marker-FP (Word 97 Macro Virus): This is a variant of the WM97/Marker-A Word macro virus. This virus changes the Word Application Username to "JonMMx2000," the user initials to "MeMeX," and the user address to "JonMMx2000@yahoo.com." On Mondays, it will create the file jon.html in the directory in which Windows is installed. This HTML file is harmless.

WM97/Myna-Fam (Word 97 Macro Virus): The majority of the viruses in the WM97/Myna family contain no intentionally malicious code. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for the presence of the virus. If the minute value of the system clock is equal to the day value, then one of the variants of the WM97/Myna family may add ten pentagons into the active document, in random colors and sizes.

WM97/Wrench-Q (Word 97 Macro Virus): This is a Word macro virus which displays the Office Assistant if you try to open the VB Editor, change the document font, or print the document. The file "ascii.vxd," containing the virus code, is dropped in the root directory.

WM97/Wrench-T (Word 97 Macro Virus): This is a Word macro virus. It displays the Microsoft Office Assistant if you try to open the Visual Basic Editor, change the document font, or print the current document. The virus drops the file "ascii.vxd" into the root directory. This file contains the virus code.

Win32.Yerg (Win32 Worm): This is a harmless, non-memory, resident, parasitic, encrypted Win32 virus. It searches for Win32 EXE applications (PE EXE files) with .EXE and .SCR file name extensions, then infects them. Upon being run from the A: drive (floppy disk), the virus looks for victim files in the Windows system directory and in all parent directories; and upon being run from any other drive, the virus looks for files in the current directory and in all parent directories, then on the A: drive. While infecting, the virus writes itself to the end of the file.

Worm.Bumerang (Win32 Worm): This is a very dangerous Win32 worm virus. The virus itself is Windows PE EXE file about 23Kb in length (compressed by UPX, with a decompressed size about 52K), and written in Microsoft Visual C++. It spreads via the local network, and infects Win32 EXE applications (PE EXE files) there. While infecting, the virus moves a file beginning to the file end, then writes itself to the beginning of the file. As a result, when an infected file is started, the virus code takes control.

WORM_PETTICK.A (Aliases: PETTICK.A, W32/PetTick@MM, W95.Pet_Tick.gen) (Worm): This UPX compressed worm propagates via MIRC and e-mail. The worm sends itself as an attachment, ANTHRAX_INFO.EXE in e-mails it sends out and to users in a channel where the infected user is connected. The e-mail arrives with the subject line: "What is Anthrax?" This worm has no destructive payload.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Adshow	N/A	CyberNotes-2001-17
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Asylum	N/A	CyberNotes-2001-18
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14
Backdoor.Darkirc	N/A	CyberNotes-2001-15
Backdoor.Darksun	N/A	CyberNotes-2001-21
Backdoor.Destiny	N/A	CyberNotes-2001-21
Backdoor.G_Door	N/A	CyberNotes-2001-18
Backdoor.IRC.Critical	N/A	CyberNotes-2001-19
Backdoor.IRC.Flood	N/A	CyberNotes-2001-16
Backdoor.KWM	N/A	CyberNotes-2001-21
Backdoor.Litmus	N/A	CyberNotes-2001-21
Backdoor.MiniCommander:	N/A	CyberNotes-2001-16
Backdoor.Oblivion	N/A	CyberNotes-2001-22
Backdoor.Penrox	N/A	CyberNotes-2001-17
Backdoor.Slackbot.B	N/A	CyberNotes-2001-21
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.Teste	N/A	CyberNotes-2001-16
Backdoor.Way	N/A	CyberNotes-2001-18
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13

Trojan	Version	CyberNotes Issue #
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	N/A	CyberNotes-2001-15
Bat.Hexvirus.1414	N/A	CyberNotes-2001-15
Bat.PG94.3964	N/A	CyberNotes-2001-15
BAT_FORMATC.K	N/A	CyberNotes-2001-13
CodeRed II	II	CyberNotes-2001-16
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
DonaldD.Trojan.C	N/A	CyberNotes-2001-19
EIC.Trojan	N/A	CyberNotes-2001-14
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
Gribble	N/A	CyberNotes-2001-19
HackTack	N/A	CyberNotes-2001-18
IRC/FinalBot	N/A	CyberNotes-2001-18
J_PWS.REDNECK	N/A	CyberNotes-2001-22
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.Alert.Trojan	N/A	CyberNotes-2001-19
JS.Seeker.B	N/A	CyberNotes-2001-18
JS_EXCEPTION.C	N/A	CyberNotes-2001-21
JS_OFFENSIVE.A	N/A	CyberNotes-2001-17
JS_SEEKER.W:	**N/A**	**Current Issue**
JS_ZOPA.A	N/A	CyberNotes-2001-14
KillMBR.g	N/A	CyberNotes-2001-16
Lil Witch FTP	1.0	CyberNotes-2001-19
MoSucker	**N/A**	**Current Issue**
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
Phoenix	2.1.28	CyberNotes-2001-18
Phreak	N/A	CyberNotes-2001-22
PWS.Cain.dr	N/A	CyberNotes-2001-19
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
QDel172	N/A	CyberNotes-2001-17
Remote Shell Trojan	N/A	CyberNotes-2001-19
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
Septer.Trojan	N/A	CyberNotes-2001-21
Shake.Trojan	N/A	CyberNotes-2001-20
StealVXS	N/A	CyberNotes-2001-17
Troj/PsychwardB	N/A	CyberNotes-2001-14
Troj/Slack	N/A	CyberNotes-2001-14
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_ALLGRO.A	N/A	CyberNotes-2001-17
TROJ_ANSET.B	N/A	CyberNotes-2001-22
TROJ_APOST.A	N/A	CyberNotes-2001-18
TROJ_BADY	N/A	CyberNotes-2001-15
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11

Trojan	Version	CyberNotes Issue #
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DSNX.A	N/A	CyberNotes-2001-17
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_HAI.A	N/A	CyberNotes-2001-17
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_ICMPBOMB.A	N/A	CyberNotes-2001-17
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_INVALID.A	N/A	CyberNotes-2001-18
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JESTRO.A	N/A	CyberNotes-2001-20
TROJ_KALM.A.SVR	N/A	CyberNotes-2001-21
TROJ_KEYLOG.25	N/A	CyberNotes-2001-17
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MODNAR.A	N/A	CyberNotes-2001-17
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MUSTARD.A	N/A	CyberNotes-2001-19
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NEWPIC.A	N/A	CyberNotes-2001-17
TROJ_NEWSAGENT.A	N/A	CyberNotes-2001-16
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_OPTIX.SVR	N/A	CyberNotes-2001-17
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_RUSH.A	N/A	CyberNotes-2001-21
TROJ_SIRCAM.A	N/A	CyberNotes-2001-15
TROJ_SPYBOY.A	N/A	CyberNotes-2001-18
TROJ_UCON.A	N/A	CyberNotes-2001-21
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VOTE.A	A	CyberNotes-2001-19
TROJ_VOTE.B	B	CyberNotes-2001-20
TROJ_VOTE.C	C	CyberNotes-2001-20
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WHISTLER.A	N/A	CyberNotes-2001-19
TROJ_ZERAF.A	N/A	CyberNotes-2001-18
Trojan.Assault.10	10	CyberNotes-2001-15
Trojan.Bat.Live4:	N/A	CyberNotes-2001-16
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	N/A	CyberNotes-2001-15
Trojan.JS.Clid.gen	N/A	CyberNotes-2001-17
Trojan.JS.Cover	N/A	CyberNotes-2001-18
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.Offensive	N/A	CyberNotes-2001-17
Trojan.Pounds	N/A	CyberNotes-2001-18
Trojan.Spy.KIM	**N/A**	**Current Issue**
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.VirtualRoot	N/A	CyberNotes-2001-16

Trojan	Version	CyberNotes Issue #
Trojan.Xtratank	N/A	CyberNotes-2001-17
Trojan.Zeraf	N/A	CyberNotes-2001-17
Trojan.ZeroBoot	N/A	CyberNotes-2001-19
VBS.AutoExec.Trojan	N/A	CyberNotes-2001-16
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Dayumi	N/A	CyberNotes-2001-22
VBS.Fiber.C	N/A	CyberNotes-2001-18
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Masteal.Trojan	N/A	CyberNotes-2001-21
VBS.Natas	N/A	CyberNotes-2001-16
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Icon	N/A	CyberNotes-2001-18
VBS.Trojan.Lariara	N/A	CyberNotes-2001-18
VBS.Zync.A	N/A	CyberNotes-2001-17
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.DpBot.Trojan	N/A	CyberNotes-2001-22
W32.JavaKiller.Trojan	N/A	CyberNotes-2001-21
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
W32.Whiter.Trojan	N/A	CyberNotes-2001-20
Y3K Rat	1.6	CyberNotes-2001-11
Zendown	N/A	CyberNotes-2001-22

JS_SEEKER.W (Aliases: SEEKER.W, JS.Trojan.Seeker-based): This encrypted Java Script Trojan changes the infected system's Internet Explorer startup page. It has no destructive payload. Upon execution, the Trojan modifies the following registry entry to change the Internet Explorer startup page of an infected system to a pornographic site:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page =
http://&ltblocked>/crackerz/

MoSucker (Alias: Backdoor.Mosucker): This is a powerful backdoor and remote access tool. When activated on an infected system, it allows more than one malicious user to connect to a system and to perform the following actions:

- Control the server - configure, restart, remove, close
- Open/Close CD-ROM tray
- Lost and kill processes
- Shutdown/restart a system
- Log activities and control mouse and keyboard
- Upload, download, run, rename of move files
- List, create, remove directories
- Control Windows interface: popup start menu, minimize all windows, show/hide system tray, hide/show Start button, change wallpaper, change resolution, change system colors, flip screen, get opened windows list
- Copy/read text from clipboard
- Open/close chat session
- Administrator of a backdoor server can control other user's rights for the server
- Play sound files
- Create log file of backdoor activities
- Send text to a printer
- Get OS system type and version
- Modify Windows Registry
- Update server from Internet

- Change date and time
- Show picture
- Steal user's ICQ info
- Get information about user's local and network drives
- Show messageboxes
- Notify a malicious user when infected user is on-line
- Get general information about infected system

The backdoor renames NETSTAT.EXE to NETSTAT.OLD when it is first activated and renames the file back when it is uninstalled. The backdoor also can install itself to the system with modification of startup keys in the Registry or INI files.

Trojan.Spy.KIM: This Trojan works under Windows. When the Trojan is executed, it installs three files to the system:

- %WinDir%\System\Krnl40.dll
- %WinDir%\heak.exe
- %WinDir%\ki.ini

It also creates a log-file named “key.dl” in the Windows directory.